VIRGINIA COMMONWEALTH UNIVERSITY

VCU

Exposure and Breach of Information

Policy Type: Administrative
Responsible Office: Office of Technology Services
Initial Policy Approved: 11/06/2014
Current Revision Approved: New Policy

Policy Statement and Purpose

In the course of conducting its academic and research functions, Virginia Commonwealth University may collect, access, transmit and store sensitive information that is protected under various federal, state and industry regulations; this information is classified as Category I information under the University Data Classification Standard. To minimize financial and reputational risks caused by the loss of Category I information, it is imperative for University employees to safeguard this information and prevent any unauthorized access, loss, or theft of this information or devices containing such information.

Whenever Virginia Commonwealth University is notified of a (potential) exposure of its Category I information, specific steps should take place to work with university officials to determine a course of action to ensure compliance with federal state, and industry regulations.

Noncompliance with this policy may result in disciplinary action up to and including termination. VCU supports an environment free from retaliation. Retaliation against any employee who brings forth a good faith concern, asks a clarifying question, or participates in an investigation is prohibited.

Table of Contents

Who Should Know This Policy

All University personnel who generate, collect, store, transmit, and process VCU Category I information should read and understand this policy.

Definitions

Affiliated Covered Entity
VCU as a HIPAA hybrid entity and VCUHS have designated themselves as an Affiliated Covered Entity (ACE), and VCU has designated certain VCU departments (or units) as required to comply with the HIPAA/HITECH standards.

Category I Information
Information protected under federal, state or industry regulations and / or other civil statutes, where if lost may require breach notification and cause potential regulatory sanctions, fines and damages to the institution's mission and reputation.

Data Custodian
The Data Custodians can have both a business and/ or technical role, though it is typically considered a business role. The Data custodians are responsible for entering, modifying and maintaining data in the enterprise databases and information systems.

Data Steward
The Data Steward is a University director or equivalent employee who oversees the capture, maintenance and dissemination of data for a particular academic or business operation. The Data Steward is responsible for ensuring data quality, develop consistent data definitions, sensitivity classifications, determine data aliases, develop standard calculations and derivations, define security requirements, document all appropriate "business rules" and monitor data quality within the source system and/or data warehouse. The Data Steward is also responsible for communicating data protection requirements to the Data Custodian; defining requirements for access to the data.

Incident
An adverse event that caused or may have caused harm to the confidentiality of sensitive university information, and/or may have led to the potential exposure of sensitive university information.

Information Exposure or Breach
Information exposure or breach refers to the unauthorized or improper access or disclosure of Category I information.

Notification
The communication of exposure or breach to the individuals affected by the information exposure or breach, as required by applicable State, Federal, or Industry regulations.

Contacts

VCU Office of Technology Services officially interprets this policy. VCU Office of Technology Services is responsible for obtaining approval for any revisions as required by the policy *Creating and Maintaining Policies and Procedures* through the appropriate governance structures. Please direct policy questions to VCU Office of Technology Services.

Procedures

Procedures establish required actions and processes to comply with a policy, support compliance with applicable laws and regulations, and mitigate risk. The following procedure outline is provided for reference, but may be changed as appropriate to best communicate the required steps.

The department responsible for the exposure should inform the department head of the incident and work with the University Information Security Office to determine appropriate action(s).

The department responsible for the exposure assumes primary responsibility for dealing with issues of the exposure according to the Virginia Commonwealth University procedure listed here. They should work with data stewards to verify the confidentiality of the data and take responsibility for working with the University insurance and risk management office, University Counsel, University Information Security Office and University relations office in developing an action plan that includes any communications, publicity, notification to individuals and others, and necessary remediation.

If deemed necessary, the group or department responsible for the information exposure or breach is responsible for coordinating with the University insurance and risk management office to contact individuals affected by the exposure of the Category I information and respond to any potential inquiries as a result to the exposure.

The following procedures should be used when handling information exposures and breach notifications.

1. **Information Exposure Handling Procedures**: The following procedure documents the steps a department must take after a potential exposure of Category I information is discovered.

    - Step 1. Once the potential information exposure is discovered, the person responsible for the discovery of the potential exposure is expected to notify the head of the department or designee responsible for the information without unreasonable delay.

    - Step 2. Upon notification, the department head or designee of the department responsible for the information should notify the information security office (infosec@vcu.edu), without unreasonable delay, about the potential information exposure, and determine whether the information in question is considered Category I information.

    - Step 3. The Information Security Office, in collaboration with the department, will coordinate initial response to the information exposure. The initial response may include the analysis of the incident leading to exposure, the containment of the exposure source, eradication of any threats that may lead to further exposure, and the recovery and restoration of services.

- Step 4. If the potentially exposed information in question is considered Category I information, the Information Security Office will coordinate the initial analysis and determine the probability of an actual exposure, and notify the department whether an information exposure is likely. Proceed to step 6 if the potentially exposed information in question is not considered Category I information.

- Step 5. If the information in question is considered Category I information and the probability of an information exposure is likely, the following steps will be followed. Otherwise, go to step 6:

    - Step 5a. Information Security Office will notify the department responsible for the information that the probability of an information exposure is likely, and notify University CIO, University Counsel, and appropriate Vice President(s) of the information exposure.

    - Step 5b. The department responsible for the information is expected to determine whether any of the following information is within scope of exposure and notify the appropriate steward(s) of the applicable information.

Information Type	**Notification Recipient**
HIPAA protected information	VCU ACE Chief Privacy Officer
HR and Payroll information	AVP of Human Resources
FERPA Protected Educational Records	Registrar
Financial Records	University Controller
Information from other data stewards	Appropriate data stewards

    - Step 5c. Additionally, the department responsible for the information is expected to notify the University Insurance and Risk Management Office as well as University Relations.

    - Step 5d. The department responsible for the information, in combination with the appropriate data stewards, the University Insurance and Risk Management Office, University Relations, and University Counsel will determine whether an information exposure or breach notification is warranted.

    - Step 5e. If it is determined that an information exposure or breach notification is warranted, the department responsible for the information will work with the Insurance and Risk Management Office to notify the individuals affected by the information exposure. Otherwise, proceed to Step 6.

- Step 6. Information Security Office will record the incident, and assist the department with any additional remediation tasks related to the incident. The department will work with Information Security Office to develop plans to prevent the reoccurrence of future incidents.

Forms

There are no forms associated with this policy and procedures.

Related Documents

Related documents are critical to the development of corresponding policies and procedures. Related documents include federal regulations, state regulations, state policies and VCU policies, procedures and guidelines.

1. Code of Virginia: Breach of Personal Information (§ 18.2-186.6)
2. Code of Virginia: Breach of Medical Information Notification (§ 32.1-127.1:05.)
3. Virginia DHRM Personnel Records Disclosure Policy (Policy number 6.05)
4. Virginia DHRM Personnel Records Management Policy (Policy Number 6.10)
5. Health Insurance Portability and Accountability Act (HIPAA)
6. Health Information Technology for Economic and Clinical Health Act (HITECH)
7. Family Educational Rights and Privacy Act (FERPA)
8. VCU Data Classification Standard
9. Information Exposure or Breach Handling Procedure Flow Chart

Revision History

This policy supersedes the following archived policies:

None – New Policy

FAQs

Q: What is considered Category I information?

A: Information containing the following data elements are considered Category I information. For a full explanation on information and data classification, please see the VCU Data classification standard.

- First name or first initial and last name in combination with and linked to any one or more of:
  - Social Security Number
  - Driver's license number or State issued ID number in lieu of driver's license number
  - Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts.

    - Any information related to an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional.
    - An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.
- Protected Health Information as defined by HIPAA
- Student Financial AID information protected under Gramm-Leach-Bliley Act
- Student Educational Records as defined by FERPA (Excluding Directory Information)
- Export controlled information regulated under ITAR, EAR, or OFAC
- COVA Identification Number (BES ID)
- Employee and personnel records protected by Virginia DHRM Policies
- Other regulated information that if lost or stolen may require breach notifications and lead to fines

Q: What is considered an incident?

A: Examples of incidents may include but are not limited to:

- A lost or stolen laptop, Smart Phone, thumb drive or other electronic storage device that is unencrypted.
- Successful hacking and intrusion against an IT system.
- Loss or theft of paper records.
- Loss or theft of user account credentials that allow an individual to access protected data without authorization.
- Public posting of sensitive information on the Internet.
- Internal fraud involving the sale or trafficking of personal information.
- Publication of sensitive information on publicly accessible paper or document
- Unauthorized interception of unencrypted information in transmission